EXHIBIT B

APPENDIX J
Cybersecurity policy

Table of Contents

Objective

The focus of this policy is to help the City of Newberg define and meet cyber security objectives. We recognize that information and the protection of information is required to serve our employees and citizens. We seek to ensure that appropriate measures are implemented to protect this information. This Cybersecurity Policy is designed to establish a foundation for an organizational culture of security. Updates to this policy will be recommended to the City Manager by the IT Director as necessary.

The purpose of this policy is to clearly communicate the City of Newberg security objectives and guidelines to minimize the risk of internal and external threats while taking advantage of opportunities that promote our objectives.

This policy applies, to all City of Newberg elected officials, employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by the City of Newberg. The IT Director has responsibility for the implementation of this policy. Department heads must ensure that all contracts and similar agreements with business partners and service providers incorporate appropriate policy elements.

Compliance

Oregon public entities must comply with the Oregon Identity Theft Protection Act, ORS 646A.600 – 628. ORS 646A.622 (d) requires the implementation of a Cybersecurity program. Non-compliance with this policy may pose risks to the organization; accordingly, compliance with this program is mandatory. Failure to comply may result in failure to obtain organizational objectives, legal action, fines and penalties. Breaches with the potential to impact more than 250 individuals must be reported to the Oregon Department of Justice.https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/

Employees who violate standards and requirements of this policy may be subject to disciplinary action up to and including termination.

Roles and Responsibilities

The City of Newberg has appointed the following roles and responsibilities to execute and monitor the policies described in this document.

- Ensure that a written Cybersecurity Policy is adopted and implemented.
- Confirm identification, acquisition, and implementation of information system software and hardware.
- Identify all Personally Identifiable Information as defined in the following table.
- Ensure implementation, enforcement, and effectiveness of IT Security policies and procedures.
- Facilitate an understanding of security at all organizational levels
- Deploy communication and training that involves all staff to build awareness of information technology security.

- Oversee daily activities and use of information systems to ensure employees, business partners, and contractors adhere to these policies and procedures.

Employees and Contractors: See Appendix A - Acceptable Use Policy

Identify, Protect, Detect, Respond, and Recover

The following sections outline City of Newberg requirements and minimum standards to facilitate the secure use of organizational information systems. The information presented in this policy follows the format of the control families outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF): ***Identify, Protect, Detect, Respond, and Recover***.

The scope of security controls addressed in this policy focus on the activities most relevant to the City of Newberg as defined by the Center for Internet Security (CIS), and industry best practices. Management and implementation of this policy is the responsibility of the IT Director.

Identify (ID)

Objective: To develop the organization's understanding that it is necessary to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Asset Management

An inventory of all approved hardware and software on the City of Newberg network and systems will be maintained in a computer program or spreadsheet that documents the following:

- The employee in possession of the hardware or software.
- Date of purchase.
- Amount of purchase.
- Serial number.
- Type of device and description.

A policy for the receipt and transfer of City laptops and phones will be developed by IT and individual acknowledgements will be held in personnel files.

Personally Identifiable Information (PII)

An inventory of all PII information by type and location will be taken. The following table may be useful to inventory PPI.

Location	PII by type	Essential	Location	Owner
Website				
Contractors				
File in staff office				
File in building				
File offsite				
Desk top				
HR System				
Financial System				
Laptop				
Flash drive				
Cell phones				
Tablets				
Other				

Each department head will determine if PII is ***essential***. If PII is not essential, it will either not be collected, or (if collected) will be destroyed. Do not collect sensitive information, such as a Social Security numbers, if there is no legitimate business need. If this information does serve a need, apply your entity's record retention plan that outlines what information must be kept, and dispose of it securely once it is no longer required to be maintained.

When records containing PII are disposed of they shall be shredded if in paper form or destroyed by IT if in electronic form.

The Oregon Identity Theft Protection Act prohibits anyone (individual, private or public corporation, or business) who maintains Social Security numbers from:

- Printing a consumer's SSN on any mailed materials not requested by the consumer unless redacted
- Printing a consumer's SSN on a card used by the consumer that is required to access products or services
- Publicly posting or displaying a consumer's SSN, such as on a website

Exceptions include requirements by state or federal laws, including statute records (such as W2s, W4s, 1099s, etc.) that are required by law to be made available to the public, for use for internal verification or administrative processes, or for enforcing a judgment or court order.

Protect (PR)

Objective: To develop and implement appropriate safeguards to ensure the delivery of critical services.

Identity Management, Authentication and Access Control

The IT Director is responsible for ensuring that access to the organization's systems and data is appropriately controlled. All systems housing City of Newberg data (including laptops, desktops, tablets, and cell phones) are required to be protected with a password or other form of authentication. Users with access to City of Newberg systems and data are not to share passwords with anyone.

The City of Newberg has established the following password configuration requirements for all systems and applications (where applicable):

- Minimum password length: 8 characters
- Password complexity: requires alphanumeric and special characters
- Prohibited reuse for Ten (10) iterations
- Changed periodically every 90 days
- Invalid login attempts set to five
- Automatic lock due to inactivity = 20 minutes

Other potential safeguards include:

- Not allowing PII on mobile storage media
- Locking file cabinets
- Not allowing PII left on desktops
- Encrypting sensitive files on computers
- Requiring password protection
- Implementing the record retention plan and destroying records no longer required

Where possible, multi-factor authentication will be used when users authenticate to the organization's systems.

- Users are granted access only to the system data and functionality necessary for their job responsibilities.
- Privileged and administrative access is limited to authorized users who require escalated access for their job responsibilities and where possible will have two accounts: one for administrator functions and a standard account for day to day activities.
- All user access requests must be approved by the IT Director.
- It is the responsibility of the HR Director to ensure that all employees and contractors who separate from the organization have all system access removed within 1 business day.

On an annual basis, a review of user access will be conducted under the direction of the IT Director to confirm compliance with the access control policies outlined above.

Awareness and Training

City of Newberg personnel are required to participate in security training in the following instances:

1. All new hires are required to complete security awareness training during orientation. Documentation of completion of this orientation will be provided to HR for the personnel file.
2. Formal security awareness refresher training is conducted on an annual basis. All employees are required to participate in and complete this training.

Upon completion of training, participants will review and sign the ***Acceptable Use Policy*** included in Appendix A which will also be maintained in the employees' personnel file.

Throughout the year, the City of Newberg will conduct email phishing exercises of its users. The purpose of these tests is to help educate users on common phishing scenarios. It will assess their level of awareness and comprehension of phishing, understanding and compliance with policies around safe handling of e-mails containing links and/or attachments, and their ability to recognize a questionable or fraudulent message.

Data Security

Data Classification

You must adhere to your departmental Records Retention Policy regarding the storage and destruction of data. Data residing on corporate systems must be continually evaluated and classified into the following categories:

- **Employees Personal Use**: Includes individual user's personal data, emails, documents, etc. This policy excludes an employee's personal information, so no further guidelines apply. As a reminder the city's equipment and software is to be used for business purposes only.
- **Marketing or Informational Material**: Includes already-released marketing material, commonly known information, data freely available to the public, etc. There are no requirements for public information.
- **Operational**: Includes data for basic organizational operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.
- **Confidential:** Any information deemed confidential. The following list provides guidelines on what type of information is typically considered confidential. Confidential data includes but is not limited to:

    - Employee or customer Social Security numbers or personally identifiable information (PII)
    - Personnel files
    - Medical and healthcare information
    - Protected Health Information (PHI)
    - Network diagrams and security configurations

- Communications regarding legal matters
- Passwords/passphrases
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)
- Criminal justice information

Data Storage

The following guidelines apply to storage of the different types of organizational data.

- **Operational:** Operational data should be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). Some type of system- or disk-level redundancy is encouraged.
- **Confidential**: Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored in a physically secure location or under lock and key (or keycard/keypad), with the key, keycard or code secured.

Data Transmission

The following guidelines apply to the transmission of the different types of organizational data.

- **Confidential**: Confidential data must not be:
  - Transmitted outside the organization's network without the use of strong encryption,
  - Left on voicemail systems, either inside or outside the organization's network.

Data Destruction

1.0 Purpose

The purpose of this policy is to outline the proper disposal of media (physical or electronic) at the City of Newberg. These rules are in place to protect confidential, sensitive, and classified information, employees and the City of Newberg. Inappropriate disposal of City of Newberg information and media may put employees and the City of Newberg at risk.

2.0 Scope

This policy applies to all City of Newberg employees, contractors, temporary staff, and other workers at the City of Newberg, with access to systems and/or data, sensitive and classified data, confidential data, and media. This policy applies to all equipment that processes, stores, and/or transmits classified and confidential data that is owned or leased by the City of Newberg.

3.0 Policy

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit classified and confidential data shall be properly disposed of in accordance with measures established by the City of Newberg.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

1) Shredding using City of Newberg issued shredders.
2) Placed in locked shredding bins for Iron Mountain to come on-site and shred, witnessed by City of Newberg personnel throughout the entire process.
3) Incineration using Covanta incinerators or witnessed by City of Newberg personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) shall be disposed of by one of the following methods:

1) **Overwriting (at least 3 times)** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
2) **Degaussing -** a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.
3) **Destruction –** a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, drilling, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems and other equipment that has been used to process, store, or transmit confidential information shall not be released from the City of Newberg's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

Data Storage

Stored Data includes any data located on organization-owned or organization-provided systems, devices, media, etc. Examples of encryption options for stored data include:

- Whole disk encryption
- Encryption of partitions/files
- Encryption of disk drives
- Encryption of personal storage media/USB drives
- Encryption of backups
- Encryption of data generated by applications

Data while transmitted includes any data sent across the organization network or any data sent to or from an organization-owned or organization-provided system. Types of transmitted data that shall be encrypted include:

- VPN tunnels
- Remote access sessions
- Web applications
- Remote desktop access
- Communications with applications/databases

Information Protection Processes and Procedures

Secure Software Development

Where applicable, all software development activities performed by the City of Newberg or by vendors on behalf of the organization shall employ secure coding practices including those outlined below.

A minimum of three software environments for the development of software systems should be available – development, quality assurance, and a production environment. Software developers or programmers are required to develop in the development environment and promote objects into the quality assurance and production environments. The quality assurance environment is used for assurance testing by the end user and the developer. The production environment should be used solely by the end user for production data and applications. Compiling objects and the source code is not allowed in the production environment. The information technology manager or an independent peer review will be required for promotion objects into the production environment.

- All production changes must be approved before being promoted to production.
- Developers should not have the ability to move their own code.
- All production changes must have a corresponding help desk change request number.
- All production changes must be developed in the development environment and tested in the quality assurance environment.
- All emergency changes must be adequately documented and approved.

Software code approved for promotion will be uploaded by the Systems administrator to the production environment from the quality assurance environment once the change request is approved. The Systems administrator may work with the developer to ensure proper placement of objects into production.

Contingency Planning

The organization's business contingency capability is based upon local backups of all business data. Full data backups will be performed on a weekly basis. Confirmation that backups were performed successfully will be conducted monthly.

During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the City Manager.

The following business contingency scenarios have been identified along with the intended responses:

- In the event that one or more of the City of Newberg's systems or applications are deemed corrupted or inaccessible, the IT Director will work with the respective vendor(s) to restore data from the most recent backup and, if necessary, acquire replacement hardware.

- In the event that the location housing the City of Newberg systems are no longer accessible, the IT Director will work with the respective vendor(s) to acquire any necessary replacement hardware and software, implement these at one of the organization's other sites, and restore data from the most recent backup.

Network Infrastructure

The organization will protect the corporate electronic communications network from the Internet by utilizing a firewall. For maximum protection, the corporate network devices shall meet the following configuration standards:

- Vendor recommended, and industry standard configurations will be used.
- Changes to firewall and router configurations will be approved by the IT Director.
- Both router and firewall passwords must be secured and difficult to guess.
- The default policy for the firewall for handling inbound traffic should be to block all packets and connections unless the traffic type and connections have been specifically permitted.
- Inbound traffic containing non-expected ICMP (Internet Control Message Protocol) traffic should not be passed in from the Internet, or from any un-trusted external network.
- All web services running on routers must be disabled.
- Simple Network Management Protocol (SNMP) Community Strings must be changed from the default "public" and "private".

Network Servers

Servers typically accept connections from several sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk associated with that system, so it is particularly important to secure network servers. The following statements apply to the organization's use of network servers:

- Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.

- Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.
- If possible, a standard installation process should be developed for the organization's network servers. A standard process will provide consistency across servers no matter what employee or contractor handles the installation.
- Clocks on network servers should be synchronized with the organization's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

Network Segmentation

Network segmentation is used to limit access to data within the City of Newberg network based upon data sensitivity. The City of Newberg maintains multiple wireless networks. The *guest* wireless network is password protected, and proper authentication will grant the user internet access only. Access to the *secure* wireless network is limited to City of Newberg employees and contractors and provides the user access to the intranet.

Protective Technology

Email Filtering

A good way to mitigate email related risk is to filter it before it reaches the user so that the user receives only safe, business-related messages. The City of Newberg will filter email at the Internet gateway and/or the mail server. This filtering will help reduce spam, viruses, or other messages that may be deemed either contrary to this policy or a potential risk to the organization's IT security.

Additionally, E-mail scanning has been implemented to identify and quarantine emails that are deemed suspicious. This functionality may or may not be used at the discretion of the IT Director.

Network Vulnerability Assessments

On an annual basis, the City of Newberg will perform both internal and external network vulnerability assessments. The purpose of these assessments is to establish a comprehensive view of the organization's network as it appears internally and externally. These evaluations will be conducted under the direction of the IT Director to identify weaknesses with the network configuration that could allow unauthorized and/or unsuspected access to the organization's data and systems.

Detect (DE)

Definition: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Anomalies and Events

The following logging activities are conducted by the Network Engineer under the direction of the IT Director:

- Domain Controllers - Active Directory event logs will be configured to log the following security events: account creation, escalation of privileges, and login failures.
- Application Servers - Logs from application servers (e.g., web, email, database servers) will be configured to log the following events: errors, faults, and login failures.
- Network Devices - Logs from network devices (e.g., firewalls, network switches, routers) will be configured to log the following events: errors, faults, and login failures.

Passwords should not be contained in logs.

Logs of the above events will be reviewed by the Network Engineer at least once per week. Event logs will be configured to maintain a record of the above events for three months.

Security Continuous Monitoring

Anti-Malware Tools

All organization servers and workstations will utilize Eset to protect systems from malware and viruses. Real-time scanning will be enabled on all systems and weekly malware scans will be performed. A monthly review of the Eset dashboard will be conducted by the Network Engineer to confirm the status of virus definition updates and scans.

The City of Newberg utilizes various mobile device management solutions to protect mobile devices from malware and viruses.

Patch management

All software updates and patches will be distributed to all City of Newberg systems as follows:

- Workstations will be configured to install critical updates.
- Server security updates will be installed manually during scheduled maintenance windows.
- Any exceptions shall be documented.

Respond (RS)

Definition: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Response Planning

The organization's annual security awareness training shall include direction and guidance for the types of security incidents users could encounter, what actions to take when an incident is suspected, and who is responsible for responding to an incident. A security incident, as it relates to the City of Newberg's information assets, can be defined as either an electronic or physical Incident.

The IT Director is responsible for coordinating all activities during a significant incident, including notification and communication activities. They are also responsible for the chain of escalation and deciding if/when outside agencies, such as law enforcement, need to be contacted.

Electronic Incidents

This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes to a virus outbreak or a suspected Trojan or malware infection. When an electronic incident is suspected, the steps below should be taken in order.

1. Contact the IT Director or on-call IT Technician

The remaining steps should be conducted under the supervision of the IT Department.

2. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.
3. Disable the compromised account(s) as appropriate.
4. Determine exactly what happened and the scope of the incident.
5. Determine how the attacker gained access and disable it.
6. Rebuild the system, including a complete operating system reinstall.
7. Restore any needed data from the last known good backup and put the system back online.
8. Take actions, as possible, to ensure that the vulnerability will not reappear.
9. Conduct a post-incident evaluation. What can be learned? What could be done differently?

Physical Incidents

A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain organization information. All instances of a suspected physical security incident should be reported immediately to the IT Director or on-call technician.

Notification

If an electronic or physical security incident is suspected of having occurred, notification of the public or affected entities should occur.

1. Contact CIS Claims at claims@cisoregon.org.
2. Notify the State of Oregon CJIS coordinator
3. Inform your attorney
4. Complete this form if the breach involves more than 250 records.
   https://justice.oregon.gov/consumer/DataBreach/Home/Submit

Recover (RC)

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems and/or assets affected by cybersecurity events.

CIS will help with the recovery process. CIS may provide forensics services, breach coaching services, legal services, media services and assist in paying for notification expenses. The CIS claims adjuster will discuss with you the coverages and services offered by CIS.

The City Manager is responsible for managing and directing activities during an incident, including the recovery steps.

Recovery planning and processes are improved by incorporating lessons learned into future activities.

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet service providers, owners of the affected systems, victims, and vendors.

External communications should only be handled by designated individuals at the direction of the City Manager. Recovery activities are communicated to internal stakeholders, executives, and management teams.

Appendix A – Acceptable Use Policy

1.0 Overview

The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to the City of Newberg established culture of openness, trust, and integrity. The City of Newberg is committed to protecting the City of Newberg's employees, partners and the public from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet- related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, File Transfer Protocol, and National Crime Information Center access are the property of the City of Newberg. These systems are to be used for business purposes in serving the interests of the agency in the course of normal operations. Effective security is a team effort involving the participation and support of every City of Newberg employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at the City of Newberg. These rules are in place to protect the employee and the City of Newberg. Inappropriate use exposes the City of Newberg to risk including virus attacks, compromises of the network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, elected officials, volunteers, contractors, consultants, temporary staff, and other workers at the City of Newberg, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the City of Newberg.

4.0 Policy

4.1 General Use and Ownership

1. While the City of Newberg's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the City of Newberg. Because of the need to protect the City of Newberg's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the City of Newberg.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/ Extranet systems. In the absence of such policies, employees should consult their

supervisor or management.

3. The City of Newberg recommends that any information that a user considers confidential or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within the City of Newberg may monitor equipment, systems and network traffic at any time.
5. The City of Newberg reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or non-confidential, as defined by agency confidentiality guidelines. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Please review the City of Newberg's cybersecurity policy for guidance.
3. All personal computers, laptops, and workstations should be secured with password- protected screen savers with an automatic activation feature, or by logging off (control-alt-delete) when the computer is unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. All Windows based devices used by employees that are connected to the City of Newberg Internet/Intranet/Extranet, whether owned by the employee or the City of Newberg, shall be continually executing approved virus-scanning software with a current database.
6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is an employee of City of Newberg authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing City of Newberg owned resources. The list below is by no means exhaustive, but attempts to provide a frame work for activities which fall into the category of unacceptable use.

4.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Unauthorized access, copying, or dissemination of confidential information.

2. Installation of any copyrighted software for which City of Newberg or end user does not have an active license.
3. Installation of any software without preapproval and virus scan.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purpose of this policy, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
7. Port scanning or security scanning is expressly prohibited unless prior notification has been given to City of Newberg IT Department.
8. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
9. Circumventing user authentication or security of any host, network, or account.
10. Interfering with or denying service to any user other than the employee's host.
11. Using any program/script/command or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

5.0 Enforcement

Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.

Signature

I have received a copy of the organization's Acceptable Use Policy as revised and approved by the management. I have read and understood the policy.

_____ (Print your name)

_____ _____

(Signature) (Date)

Appendix B – Confidentiality and Non-Disclosure Agreement

This Confidentiality and Nondisclosure Agreement (the "Agreement") is entered into by and between **City of Newberg** ("Disclosing Party") and _____ ("Receiving Party") for the purpose of preventing the unauthorized disclosure of Confidential Information as defined below. The parties agree to enter into a confidential relationship with respect to the disclosure of certain proprietary and confidential information ("Confidential Information").

1. *Definition of Confidential Information.* For purposes of this Agreement, "Confidential Information" shall include all information or material that has or could have commercial value or other utility in the business in which Disclosing Party is engaged. Examples of Confidential Information include the following:
    - Employee or customer Social Security numbers or personal information
    - Customer data
    - Entity financial data
    - Product and/or service plans, details, and schematics,
    - Network diagrams and security configurations
    - Communications about entity legal matters
    - Passwords
    - Bank account information and routing numbers
    - Payroll information
    - Credit card information
    - Any confidential data held for a third party
2. *Exclusions from Confidential Information.* Receiving Party's obligations under this Agreement do not extend to information that is:
    a. Publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party;
    b. Discovered or created by the Receiving Party before disclosure by Disclosing Party;
    c. Learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or
    d. Is disclosed by Receiving Party with Disclosing Party's prior written approval.
3. *Obligations of Receiving Party.* Receiving Party shall hold and maintain the Confidential Information in strictest confidence for the sole and exclusive benefit of the Disclosing Party. Receiving Party shall carefully restrict access to Confidential Information to employees, contractors, and third parties as is reasonably required and shall require those persons to sign nondisclosure restrictions that are at least as protective as those in this Agreement. Receiving Party shall not, without the prior written approval of Disclosing Party, use for Receiving Party's own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of Disclosing Party, any Confidential Information. Receiving Party shall return to Disclosing Party any and all records, notes, and other written, printed, or tangible materials in its possession pertaining to Confidential Information immediately if Disclosing Party requests it in writing.

4. *Time Periods.* The nondisclosure provisions of this Agreement shall survive the termination of this Agreement and Receiving Party's duty to hold Confidential Information in confidence shall remain in effect until the Confidential Information no longer qualifies as a trade secret or until Disclosing Party sends Receiving Party written notice releasing Receiving Party from this Agreement, whichever occurs first.
5. *Relationships.* Nothing contained in this Agreement shall be deemed to constitute either party a partner, joint venture or employee of the other party for any purpose.
6. *Severability.* If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted so as best to affect the intent of the parties.
7. *Integration.* This Agreement expresses the complete understanding of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations, and understandings. This Agreement may not be amended except in a writing signed by both parties.
8. *Waiver.* The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights.

This Agreement and each party's obligations shall be binding on the representatives, assigns, and successors of such party. Each party has signed this Agreement through its authorized representative.

Disclosing Party

By: _____

Printed Name: _____

Title: _____

Dated: _____

Receiving Party

By: _____

Printed Name: _____

Title: _____

Dated: _____